Discrete Applied Mathematics 47 (1993) 233–249
North-Holland

Trace-orthogonal normal bases

Dieter Jungnickel

Lehrstuhl für Angewandte Mathematik II, Universität Augsburg, D-86135 Augsburg, Germany

Received 7 May 1991
Revised 12 September 1991

Abstract

In this paper, we shall first obtain some basic theoretical results on trace-orthogonal normal bases of $GF(q^n)$ over $GF(q)$: We show that such a basis exists if and only if a self-dual normal basis exists (in fact, any such basis is equivalent to a self-dual one) and we give several characterizations of the trace-orthogonal normal bases in terms of two matrices M and T (associated with every normal basis N) describing the multiplicative structure of $GF(q^n)$. The matrix T is actually the matrix used in investigating the complexity of the normal basis N. Using this fact, we also completely determine the trace-orthogonal optimal normal bases. In the special case $q = 2$, n even, we then give a simple construction associating with every self-dual normal basis N another such basis N^* and relate the complexities of these two bases. This allows us to obtain an upper bound on the complexity of self-dual normal bases in this case which turns out to explain several entries in the available tables on computer searches regarding the complexity of normal bases. Finally, we give a product construction for (trace-orthogonal) normal bases.

Keywords. Finite field, normal basis, self-dual basis, trace, complexity.

1. Introduction

The present paper brings together two topics in the theory of finite fields which have generated considerable interest: arithmetics using a normal basis representation, and self-dual (or, slightly more general, trace-orthogonal) normal bases. (For background on finite fields, the reader is referred to Lidl and Niederreiter [14]; also, the required definitions will be recalled below.) As we shall see, there are some interesting (and somewhat surprising) connections between these notions. Both notions have important applications, e.g. in the construction of devices for the arithmetic in finite fields (multiplication, exponentiation, discrete logarithms) and in applications to coding theory, cryptography and the discrete Fourier transform (see [0, 1, 3, 6–9, 15, 17, 20]).

Throughout this paper, E will denote the n-dimensional extension $GF(q^n)$ of a finite field $F = GF(q)$. Now let $B = \{\alpha_0, \ldots, \alpha_{n-1}\}$ be any basis of E/F. Then the multiplication

Correspondence to: Professor D. Jungnickel, Lehrstuhl für Angewandte Mathematik II, Universität Augsburg, D-86135 Augsburg, Germany.

in E is determined by n symmetric bilinear forms $f_0, \ldots, f_{n-1}: E \times E \to F$, where $f_i(\xi, \eta)$ is the coefficient of α_i in the product $\xi\eta$. Clearly, one may compute the matrices M_i $(i = 0, \ldots, n-1)$ of these bilinear forms with respect to B as soon as one knows how to express the products of any two elements of B in terms of B. Massey and Omura [15] observed that the knowledge of just one of these forms suffices if one uses for B a *normal basis* for E/F, i.e. any basis of the form

$$\alpha_0 := \alpha, \alpha_1 := \alpha^q, \ldots, \alpha_{n-1} := \alpha^{q^{n-1}}. \tag{1.1}$$

We note that the elements of the normal basis N (we shall usually denote normal bases by the letter N) generated by α are just the conjugates of α under the Galois group G of E/F. It is now easily checked that one has

$$f_i(\xi, \eta) = f_0(\xi^{q^{n-i}}, \eta^{q^{n-i}}) \tag{1.2}$$

for $i = 0, \ldots, n-1$ and for all $\xi, \eta \in E$. Thus all the information required to perform multiplication in terms of the normal basis N generated by α is contained in the matrix $M = M_0$ representing f_0 with respect to the basis B. (Of course, the choice of the index 0 as the "fundamental" index in (1.2) is arbitrary, but – as we shall see below – particularly useful.) The element α in (1.1) is called a *normal basis generator* of E/F.

There is an alternative way of describing the multiplication in E when using a normal basis N. Because of the transitivity of G on N, the products of any two basis elements (and thus arbitrary products) are already determined once we can express the product of any basis element with α, i.e. the n elements α^{q^i+1} $(i = 0, \ldots, n-1)$, in terms of N. We now introduce some notation. Given any element ξ of E, we write $r(\xi)$ for the row vector of coordinates of ξ with respect to N:

$$r(\xi) = (x_0, \ldots, x_{n-1}) \quad \Leftrightarrow \quad \xi = x_0\alpha_0 + \cdots + x_{n-1}\alpha_{n-1}. \tag{1.3}$$

We also introduce two more functions which will be required later:

$$\sigma(\xi) := x_0 + \cdots + x_{n-1}, \qquad w(\xi) := |\{i: x_i \neq 0, i = 0, \ldots, n-1\}|. \tag{1.4}$$

Thus all the information required to perform multiplication in terms of the normal basis N generated by α is also contained in the following matrix T:

$$T := \begin{pmatrix} r(\alpha^2) \\ r(\alpha^{q+1}) \\ \vdots \\ r(\alpha^{q^{n-1}+1}) \end{pmatrix} = \begin{pmatrix} r(\alpha\alpha_0) \\ r(\alpha\alpha_1) \\ \vdots \\ r(\alpha\alpha_{n-1}) \end{pmatrix}. \tag{1.5}$$

In other words, the entry t_{ij} $(i, j = 0, \ldots, n-1)$ of T is the coefficient of $\alpha_j = \alpha^{q^j}$ in the representation of $\alpha\alpha_i = \alpha^{q^i+1}$ with respect to N. It is not difficult to show that the matrix M corresponding to the Massey–Omura approach and the matrix T just defined are related as follows:

$$m_{ij} = t_{i-j,-j} \quad \text{for all } i, j = 0, \ldots, n-1. \tag{1.6}$$

(This has been observed by Menezes [16]; it is essentially also contained in Geiselmann and Gollmann [8] who only consider the special case $q = 2$ and use the matrix M' belonging to the bilinear form f_{n-1} instead.)

Following Mullin, Onyszchuk, Vanstone and Wilson [20], the *complexity* C_N of the normal basis N generated by α is the number of nonzero entries of T (or of M), i.e.

$$C_N = w(\alpha\alpha_0) + w(\alpha\alpha_1) + \cdots + w(\alpha\alpha_{n-1}). \tag{1.7}$$

In the special case where $q = 2$, the complexity of N determines the number of gates required for a hardware realization of multiplication in E using a Massey–Omura multiplier (see [15]) based on the normal basis N: One needs precisely C_N AND-gates and $C_N - 1$ XOR-gates. This led to the search for normal bases with low complexity. We note that such bases can also be useful in software implementations of finite field arithmetics, cf. [16] and [17]. Hence there has been considerable interest in constructing normal bases of low complexity, see [2, 5, 20, 21]. The following lower bound on the complexity was obtained in [20].

Result 1.1. *Any normal basis N of* $\mathrm{GF}(q^n)/\mathrm{GF}(q)$ *satisfies*

$$C_N \geq 2n - 1. \tag{1.8}$$

In view of this result and of the preceding remarks, a normal basis achieving equality in (1.8) is called an *optimal* normal basis. All the known optimal normal bases are provided by the following two constructions due to Mullin, Onyszchuk, Vanstone and Wilson [20].

Result 1.2. *Let $n + 1$ be a prime, and assume that q is a primitive root modulo $n + 1$. Then the cyclotomic polynomial Φ_{n+1} is irreducible over* $\mathrm{GF}(q)$ *and its roots form an optimal normal basis of* $\mathrm{GF}(q^n)$ *over* $\mathrm{GF}(q)$.

Result 1.3. *Let $2n + 1$ be a prime, and assume that either*

$$2 \text{ is a primitive root modulo } 2n + 1 \tag{1.9}$$

or

$$2n + 1 \equiv 3 \bmod 4 \text{ and } 2 \text{ generates the quadratic residues modulo } 2n + 1. \tag{1.10}$$

Then there exists an optimal normal basis for $\mathrm{GF}(2^n)$ *over* $\mathrm{GF}(2)$ *which is constructed as follows: One chooses a primitive $(2n + 1)$-st root of unity ζ over* $\mathrm{GF}(q)$; *then $\alpha = \zeta + \zeta^{-1}$ generates the desired basis.*

We note that all the optimal normal bases of Result 1.3 have *distribution* $(1, n - 1, 0, \ldots, 0)$. This means the following: $n - 1$ of the n products $\alpha\alpha_i$ have weight two, and the remaining one has weight 1. Recently, Mullin [19] gave the following characterization of the bases provided by Result 1.3.

Result 1.4. $\mathrm{GF}(q^n)/\mathrm{GF}(q)$ *has an optimal normal basis* N *with distribution* $(1, n-1, 0, \ldots, 0)$ *if and only if* q *is even and* N *is equivalent to one of the optimal normal bases constructed in Result* 1.3.

We next discuss the known results about self-dual normal bases. First we recall the definition of the *trace* function from E to F:

$$\mathrm{Tr}_{E/F}(\xi) = \sum_{k=0}^{n-1} \xi^{q^k}. \tag{1.11}$$

If we represent ξ in terms of the normal basis generated by α, we obtain a particularly simple expression for the trace in terms of the function σ introduced in (1.4):

$$\mathrm{Tr}(\xi) = \sigma(\xi)\,\mathrm{Tr}(\alpha). \tag{1.12}$$

Thus it suffices to compute $\mathrm{Tr}(\alpha)$ in order to determine all traces. (We omit the suffix E/F as long as it is clear which fields E and F are involved.)

It is well known that the mapping $\tau: E \times E \to F$ defined by $\tau(\alpha, \beta) := \mathrm{Tr}_{E/F}(\alpha\beta)$ is a nondegenerate bilinear form on E, the *trace bilinear form.* Given any basis $B = \{\alpha_0, \ldots, \alpha_{n-1}\}$ of E/F, there exists a unique *dual* basis $C = \{\gamma_0, \ldots, \gamma_{n-1}\}$ satisfying $\mathrm{Tr}(\alpha_i \gamma_j) = \delta_{ij}$ for all $i, j = 0, \ldots, n-1$; if B is a normal basis, so is C. We shall need the following well-known basic fact about dual bases.

Result 1.5. *Let* $B = \{\alpha_0, \ldots, \alpha_{n-1}\}$ *and* $C = \{\gamma_0, \ldots, \gamma_{n-1}\}$ *be a pair of dual bases of* $\mathrm{GF}(q^n)/\mathrm{GF}(q)$, *and let* ξ *be any element of* $\mathrm{GF}(q^n)$. *Then the coordinate of* α_i *in the representation of* ξ *with respect to* B *equals* $\mathrm{Tr}(\xi\gamma_i)$.

One calls B a *self-dual* basis of E/F if it coincides with its dual basis; slightly more generally, one calls B a *trace-orthogonal* basis if $\mathrm{Tr}(\alpha_i \alpha_j) = 0$ whenever $i \neq j$ (then the elements of the dual basis are of the form $\gamma_i = x_i \alpha_i$ for suitable elements $x_i \in F$, $i = 0, \ldots, n-1$). Of course, these two notions coincide when $q = 2$. Lempel and Weinberger [13] have obtained the following criterion for the existence of a self-dual normal basis of E/F.

Result 1.6. *A self-dual normal basis of* $\mathrm{GF}(q^n)/\mathrm{GF}(q)$ *exists if and only if either*

$$q \text{ is even and } n \text{ is not a multiple of } 4 \tag{1.13}$$

or

$$\text{both } q \text{ and } n \text{ are odd.} \tag{1.14}$$

We can now describe the results obtained in the present paper. In Section 2, we shall show that the same existence criterion as in Result 1.6 also applies for trace-orthogonal normal bases; in fact, any such basis is equivalent to a self-dual normal basis. (Two bases of E/F are said to be *equivalent* if they only differ by multiplication with a constant element of F.) Strengthening a result of Geiselmann and Gollmann

[8] for $q = 2$, we then show that a normal basis N is trace-orthogonal if and only if the matrix T associated with N as in (1.4) is symmetric; moreover, this happens if and only if the two matrices T and M coincide. Combining these facts with Result 1.4 then allows a complete classification of all trace-orthogonal optimal normal bases.

In Section 3, we consider elements $\gamma = a + b\alpha$, where α is a normal basis generator of E/F and where a, b are nonzero elements of F, and determine when such an element γ is also a normal basis generator. In particular, this will be true if $q = 2$ and n is even (and, of course, $a = b = 1$). This case will be considered in more detail in Section 4 where we will see that γ then generates a self-dual normal basis if and only if α does; we will then relate the complexities of these two self-dual normal bases. This allows us to obtain an upper bound on the complexity of a self-dual normal basis which quite surprisingly coincides with the maximum possible complexities given in the tables of [20] for several values of n (and allows us a theoretical construction of bases assuming this bound). Also, for $n = 30$, our approach yields a normal basis with considerably larger complexity than the bound provided by the (incomplete) computer search of [20]. Of course, bases with large complexity are of no practical interest (they are what should be avoided!), but it seems important for a deeper understanding of the properties of complexity to be able to explain the values found by computer searches in a more theoretical way.

Finally, in Section 5, we shall generalize a product construction for normal bases (and the determination of the resulting complexity) given by Séguin [21] for $q = 2$ to the case of arbitrary prime powers q and also obtain a curious formula for the behaviour of the trace function under this construction. In particular, we shall see that Séguin's construction preserves trace-orthogonality; this will allow us to explain one further value in the tables of [20].

After finishing this research, the author has obtained a copy of the (as yet unpublished) Diplomarbeit of Meyer [18]. There is some overlap between the results of Section 2 of the present paper and Meyer's work: In particular, Meyer also obtains the equivalence of trace-orthogonal and self-dual normal bases and the result that a normal basis N is trace-orthogonal if and only if the matrix T associated with N is symmetric (but not the equivalent condition that the matrices T and F coincide, since he works with F' instead of F). We note that our proofs are different from Meyer's (and, for the characterization theorem just mentioned, considerably simpler). Finally, Meyer also has the characterization of self-dual optimal normal bases over GF(2) (but not the case of general q).

2. Fundamental results on trace-orthogonal normal bases

In this section, we shall obtain some theoretical results on trace-orthogonal normal bases. For the sake of completeness, we first settle the existence question. The following result seems not to have been stated explicitly in the literature, though it is more or less immediate from the work of [12] and [13].

Theorem 2.1. *Any trace-orthogonal normal basis of* $\mathrm{GF}(q^n)/\mathrm{GF}(q)$ *is equivalent to a self-dual basis. Hence a trace-orthogonal normal basis exists if and only if either*

$$q \text{ is even and } n \text{ is not a multiple of } 4 \tag{2.1}$$

or

$$\text{both } q \text{ and } n \text{ are odd.} \tag{2.2}$$

Proof. Let α generate a trace-orthogonal normal basis N of $E = \mathrm{GF}(q^n)$ over $F = \mathrm{GF}(q)$, as in (1.1). With respect to N, the trace bilinear form is represented by the matrix cI, where $c = \mathrm{Tr}(\alpha^2) \neq 0$ (since the Galois group G of E/F is transitive on the elements of N). If c is a square in F, say $c = d^2$, we may obtain a generator β for an equivalent self-dual normal basis by putting $\beta = \alpha/d$. Clearly this assumption is satisfied when q is even. Now assume that q is odd. Then it has been shown in the proof of Theorem 1 in [10] (which is a simple alternative proof of the existence criterion for self-dual bases originally proved by Lempel and Seroussi [12]) that the trace bilinear form is represented (with respect to any basis) by a matrix with determinant a square in F if and only if n is odd. Since the determinant of cI is c^n, we conclude that the existence of α implies that n is odd and c is a square (so that we can construct an equivalent self-dual normal basis by the argument above). The assertion now follows from Result 1.6. □

We next give the characterization of trace-orthogonal normal bases announced in the introduction.

Theorem 2.2. *Let* α *be a generator for a normal basis* N *of* $E = \mathrm{GF}(q^n)$ *over* $F = \mathrm{GF}(q)$, *as in* (1.1), *and let* M *and* T *be the corresponding matrices defined in the introduction. Then the following conditions are equivalent:*

$$N \text{ is trace-orthogonal.} \tag{2.3}$$

$$T = M. \tag{2.4}$$

$$T \text{ is symmetric.} \tag{2.5}$$

$$\text{One has } \sigma(\alpha\alpha_0) = \mathrm{Tr}(\alpha) \text{ and } \sigma(\alpha\alpha_1) = 0 \text{ for } i = 1, \ldots, n-1, \text{ where } \sigma \text{ is the function defined in (1.4).} \tag{2.6}$$

Proof. We first assume the validity of (2.3). As in the proof of Theorem 2.1, we write $c = \mathrm{Tr}(\alpha^2) \neq 0$ and now put $\gamma_i := \alpha_i/c$ for $i = 0, \ldots, n-1$. Then we have $\mathrm{Tr}(\alpha_i \gamma_j) = \delta_{ij}$ for all $i, j = 0, \ldots, n-1$, and thus $\gamma = \gamma_0$ generates the dual normal basis $N' = \{\gamma_0, \ldots, \gamma_{n-1}\}$ of E/F. By Result 1.5, we can use the elements of N' to compute the coordinate vector of any $\xi \in F$ with respect to N. Recall that the (i,j)-entry t_{ij} of T is the coefficient of α_j in the representation of $\alpha\alpha_i$ with respect to N. We thus have

$$t_{ij} = \mathrm{Tr}(\alpha_0 \alpha_i \alpha_j)/c \tag{2.7}$$

for all $i, j = 0, \ldots, n-1$. Because of (1.6), we obtain

$$m_{ij} = t_{i-j,-j} = \mathrm{Tr}(\alpha_0 \alpha_{i-j} \alpha_{-j})/c. \tag{2.8}$$

Applying the unique Galois automorphism which maps $\alpha = \alpha_0$ to α_j to equation (2.8) gives

$$m_{ij} = \mathrm{Tr}(\alpha_j \alpha_i \alpha_0)/c = \mathrm{Tr}(\alpha_0 \alpha_i \alpha_j)/c = t_{ij},$$

i.e., the validity of (2.4).

Trivially, the validity of (2.4) implies that of (2.5), since M is a symmetric matrix. Now assume the validity of (2.5). By definition, the ith row of T is the coordinate vector $r(\alpha\alpha_i)$ of $\alpha\alpha_i$ with respect to N. Thus, the sum of all rows of T is the coordinate vector of

$$\alpha\alpha_0 + \cdots + \alpha\alpha_{n-1} = \alpha(\alpha_0 + \cdots + \alpha_{n-1}) = \alpha\,\mathrm{Tr}(\alpha),$$

i.e., the row vector

$$s = (\mathrm{Tr}(\alpha), 0, \ldots, 0). \tag{2.9}$$

In other words, s is the vector of column sums of T. Since T is symmetric, s is also the vector of row sums of T which shows the validity of condition (2.6).

Finally, assume the validity of (2.6). As noted in (1.12), we have $\mathrm{Tr}(\xi) = \sigma(\xi)\,\mathrm{Tr}(\alpha)$ for all elements ξ of E. In particular, we obtain

$$\mathrm{Tr}(\alpha\alpha_i) = \sigma(\alpha\alpha_i)\,\mathrm{Tr}(\alpha) \quad \text{for } i = 0, \ldots, n-1. \tag{2.10}$$

Because of (2.6), we immediately see that N is a trace-orthogonal basis, i.e., the validity of (2.3). □

We remark that choosing M as the matrix corresponding to the symmetric bilinear form f_0 was required for the validity of condition (2.4) above (which does not hold for the matrix M_i associated with one of the remaining f_i, though an analogous result can of course be obtained by using M_i and the matrix with kth row $r(\alpha_i\alpha_{i+k})$ $(k = 0, \ldots, n-1)$ instead of M and T, respectively). We also note the following fact about the trace function which follows from the proof of Theorem 2.2 (alternatively, it may be obtained by a simple direct computation):

Corollary 2.3. *Let α be a generator for a trace-orthogonal normal basis N of* $\mathrm{GF}(q^n)$ *over* $\mathrm{GF}(q)$. *Then one has*

$$\mathrm{Tr}(\alpha^2) = \mathrm{Tr}(\alpha)^2. \tag{2.11}$$

Moreover, $\beta = \alpha/\mathrm{Tr}(\alpha)$ generates an equivalent self-dual normal basis.

Proof. The validity of (2.11) is immediate from (2.10) and (2.6). Hence we may choose $\mathrm{Tr}(\alpha)$ for the element called d in the proof of Theorem 2.1. □

Since the most important special case for applications is the case $q = 2$ (which will be studied in more detail later), it is worthwhile to specialize Theorem 2.2 to this case.

Corollary 2.4. *Let α be a generator for a normal basis N of $E = \mathrm{GF}(2^n)$ over $F = \mathrm{GF}(2)$, as in* (1.1), *and let M and T be the corresponding matrices defined in the introduction. Then the following conditions are equivalent:*

$$N \text{ is self-dual.} \tag{2.12}$$

$$T = M. \tag{2.13}$$

$$T \text{ is symmetric.} \tag{2.14}$$

$$\text{One has } w(\alpha\alpha_0) = 1 \text{ and } w(\alpha\alpha_i) \equiv 0 \bmod 2 \text{ for } i = 1, \ldots, n-1, \text{ where } w \text{ is as in (1.4).} \tag{2.15}$$

The equivalence of (2.12) and (2.14) above was first obtained by Geiselmann and Gollmann [8] with a different proof. We note that all the optimal normal bases constructed in Result 1.3 satisfy (2.15) and are therefore self-dual. In fact, they are essentially the only trace-orthogonal optimal normal bases.

Theorem 2.5. *Let α be a generator for an optimal trace-orthogonal normal basis N of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$. Then q is even, and N is equivalent to an optimal normal basis for $\mathrm{GF}(2^n)$ over $\mathrm{GF}(2)$ as constructed in Result* 1.3. *In particular, $2n + 1$ must be a prime and n must satisfy either condition* (1.9) *or condition* (1.10).

Proof. Note that the elements $\alpha\alpha_i$ $(i = 0, \ldots, n-1)$ are linearly independent, since they arise from the basis N by multiplying every basis element by the constant element α. Since the rows of the matrix T are the coordinate vectors of the elements $\alpha\alpha_i$, they are also linearly independent. In particular, T cannot contain any zero-row. Hence condition (2.6) in Theorem 2.2 implies that each of the elements $\alpha\alpha_i$ with $i \neq 0$ has weight at least 2. Since N has complexity $2n - 1$, T has exactly $2n - 1$ entries $\neq 0$. It is now clear that the distribution of N must be $(1, n-1, 0, \ldots, 0)$. The assertion follows from Result 1.4. □

3. A simple construction for normal basis generators

Let α be a generator for a normal basis N of $E = \mathrm{GF}(q^n)$ over $F = \mathrm{GF}(q)$. Trivially, $a\alpha$ is also a normal basis generator for any $a \in F^*$. The normal bases generated by these two elements are equivalent; in particular, they have the same complexity. Another simple way of using α to construct further normal basis generators (which will, in general, lead to bases of different complexity) will now be discussed. We put $\gamma = a + b\alpha$, where a, b are nonzero elements of F, and determine when such an element γ is also a normal basis generator. As we shall see, it is almost always possible to choose suitable values of a and b. A similar result is also obtained when both normal bases are required to be trace-orthogonal.

Proposition 3.1. *Let α be a generator for a normal basis N of $E = \mathrm{GF}(q^n)$ over $F = \mathrm{GF}(q)$, as in (1.1), and let $a, b \in F^*$. Then $\gamma = a + b\alpha$ is also a normal basis generator if and only if one has*

$$na + b\,\mathrm{Tr}(\alpha) \neq 0. \tag{3.1}$$

Proof. Assume first that (3.1) is violated. Then we have

$$\mathrm{Tr}(\gamma) = \mathrm{Tr}(a + b\alpha) = na + b\,\mathrm{Tr}(\alpha) = 0$$

and thus the conjugates of γ are linearly dependent. Conversely, assume that (3.1) holds and that the conjugates $\gamma_0, \ldots, \gamma_{n-1}$ of $\gamma = \gamma_0$ are linearly dependent, say

$$x_0\gamma_0 + \cdots + x_{n-1}\gamma_{n-1} = 0, \quad \text{not all } x_i = 0. \tag{3.2}$$

Substituting for the γ_i in (3.2), we obtain

$$x_0\alpha_0 + \cdots + x_{n-1}\alpha_{n-1} = -a(x_0 + \cdots + x_{n-1})/b =: y. \tag{3.3}$$

Since we have $\alpha_0 + \cdots + \alpha_{n-1} = \mathrm{Tr}(\alpha) \neq 0$, we can also write

$$y = y\,\mathrm{Tr}(\alpha)/\mathrm{Tr}(\alpha) = (\alpha_0 + \cdots + \alpha_{n-1})y/\mathrm{Tr}(\alpha). \tag{3.4}$$

By the uniqueness of representing y with respect to the basis N, we obtain from (3.3) and (3.4) the condition

$$x_0 = \cdots = x_{n-1} = y/\mathrm{Tr}(\alpha). \tag{3.5}$$

From the definition of y in (3.3), we now see that

$$y = -a(x_0 + \cdots + x_{n-1})/b = -any/b\,\mathrm{Tr}(\alpha). \tag{3.6}$$

Since the conjugates of α are linearly independent, we have $y \neq 0$, and therefore (3.6) contradicts (3.1). This finishes the proof. □

We note that we can always choose suitable $a, b \neq 0$ such that (3.1) is satisfied, except in the case where $q = 2$ and n is odd. We now obtain a similar result when we also assume that N is actually trace-orthogonal.

Proposition 3.2. *Let α be a generator for a trace-orthogonal normal basis N of $E = \mathrm{GF}(q^n)$ over $F = \mathrm{GF}(q)$, as in (1.1), and let $a, b \in F^*$. Then $\gamma = a + b\alpha$ also generates a trace-orthogonal normal basis if and only if one has*

$$na + 2b\,\mathrm{Tr}(\alpha) = 0. \tag{3.7}$$

Proof. Note first that the validity of (3.7) implies that of (3.1), since $b\mathrm{Tr}(\alpha) \neq 0$. Hence (3.7) can only hold if γ at least generates a normal basis. Now assume this to be the case and denote the conjugates of γ by $\gamma_0, \ldots, \gamma_{n-1}$. By definition, we have

$$\gamma\gamma_i = (a + b\alpha)(a + b\alpha_i) = a^2 + ab(\alpha + \alpha_i) + b^2\alpha\alpha_i \tag{3.8}$$

and thus (as N is trace-orthogonal)

$$\mathrm{Tr}(\gamma\gamma_i) = na^2 + 2ab\,\mathrm{Tr}(\alpha) \quad \text{for } i = 1, \ldots, n-1. \tag{3.9}$$

Since $a \neq 0$, we conclude from (3.9) that the normal basis N^* generated by γ is also trace-orthogonal if and only if (3.7) holds. □

Again, we comment about the possibility of choosing $a, b \neq 0$ for which condition (3.7) is satisfied. This time, the answer depends on the characteristic p of GF(q). If $p = 2$, we can find suitable elements (e.g., $a = b = 1$) if and only if n is even. On the other hand, if p is odd, suitable elements can be selected if and only if n is not divisible by p.

We note the following immediate consequence of Propositions 3.1 and 3.2 for the case $q = 2$.

Corollary 3.3. *Let $\alpha \in \mathrm{GF}(2^n)$, where n is even, and put $\gamma = 1 + \alpha$. Then α generates a (self-dual) normal basis if and only if γ does.*

It should be noted that it is well known how one can generate all (self-dual) normal bases of $\mathrm{GF}(q^n)/\mathrm{GF}(q)$ if one such basis is known by transforming the original basis with all (orthogonal) circulant matrices in $\mathrm{GL}(n, q)$, see [4] and [10]. However, in general there is no way of relating the complexities of the original basis and of the transformed basis obtained by using a specified circulant matrix. The importance of the simple Corollary 3.3 above will be that in this special case the complexities can often be related.

4. The complexity of self-dual normal bases over GF(2)

In this section, we will first relate the complexities of two self-dual normal bases for $\mathrm{GF}(2^n)/\mathrm{GF}(2)$ generated by elements α and $\gamma = 1 + \alpha$ as in Corollary 3.3. This will allow us to obtain an upper bound for the complexity of self-dual normal bases if n is even (i.e., by Result 1.6, if $n \equiv 2 \bmod 4$). It will then be interesting to compare our results with the table in [20] for the complexity of normal bases over GF(2) with $n \leq 30$.

Theorem 4.1. *Let α generate a self-dual normal basis N for $\mathrm{GF}(2^n)/\mathrm{GF}(2)$, where n is even. Put $\gamma = 1 + \alpha$, and let N^* be the self-dual normal basis generated by γ. Then the complexities of N and N^* are related as follows:*

$$C_{N^*} = n^2 - 3n + 8 - C_N. \tag{4.1}$$

Proof. We begin with a few auxiliary observations.

$$\text{The coefficient } t_{i0} \text{ of } \alpha \text{ in } \alpha\alpha_i \text{ is 1 for } i = 1 \text{ and 0 otherwise.} \tag{4.2}$$

To see this, note that the self-duality of N implies (by Result 1.5) that the desired coefficient is $\mathrm{Tr}(\alpha^2\alpha_i) = \mathrm{Tr}(\alpha\alpha_{i-1})$. Now (4.2) follows by another application of the self-duality of N. A similar argument also shows

$$\text{the coefficient } t_{ii} \text{ of } \alpha_i \text{ in } \alpha\alpha_i \text{ is 1 for } i = n-1 \text{ and 0 otherwise.} \tag{4.3}$$

To compute the complexity of N^*, we now have to compute the weights $w(\gamma\gamma_i)$ for $i = 0, \ldots, n-1$, cf. (1.7). Trivially, we have

$$w(\gamma\gamma_0) = 1. \tag{4.4}$$

Now let $i \neq 0$. We then have

$$\gamma\gamma_i = (1+\alpha)(1+\alpha_i) = 1 + \alpha + \alpha_i + \alpha\alpha_i$$

which can be written as

$$\begin{aligned}\gamma\gamma_i = {} & (1+\alpha_0) + (1+\alpha_i) + (\alpha_0 + \cdots + \alpha_{n-1}) \\ & + (t_{i,0}\alpha_0 + \cdots + t_{i,n-1}\alpha_{n-1}),\end{aligned} \tag{4.5}$$

where we have used the facts that $\mathrm{Tr}(\alpha) = 1$ and that the coordinate vector of $\alpha\alpha_i$ with respect to N is the ith row of the matrix T associated with N. Since both n and $w(\alpha\alpha_i)$ are even (by hypothesis and by Corollary 2.4), we may rewrite (4.5) as follows:

$$\begin{aligned}\gamma\gamma_i &= (1+\alpha_0) + (1+\alpha_i) \\ &\quad + [(1+t_{i,0})(1+\alpha_0) + \cdots + (1+t_{i,n-1})(1+\alpha_{n-1})] \\ &= \gamma_0 + \gamma_i + [(1+t_{i,0})\gamma_0 + \cdots + (1+t_{i,n-1})\gamma_{n-1}].\end{aligned} \tag{4.6}$$

By (4.2) and (4.3), we have $t_{i0} = t_{ii} = 0$ if $i \neq 1, n-1$. In this case, the terms in (4.6) involving γ_0 and γ_i, respectively, cancel; hence γ_j then has coefficient 1 in (4.6) if and only if $t_{ij} = 0$ and $j \neq 0, i$. Thus we have

$$w(\gamma\gamma_i) = n - 2 - w(\alpha\alpha_i) \quad \text{for } i \neq 0, 1, n-1. \tag{4.7}$$

A similar argument shows

$$w(\gamma\gamma_i) = n - w(\alpha\alpha_i) \quad \text{for } i = 1 \text{ and for } i = n-1. \tag{4.8}$$

Substituting (4.4), (4.7) and (4.8) for the weights $w(\gamma\gamma_i)$, we obtain

$$\begin{aligned}C_{N^*} &= w(\gamma\gamma_0) + w(\gamma\gamma_1) + \cdots + w(\gamma\gamma_{n-1}) \\ &= 1 + (n - w(\alpha\alpha_1)) + (n - 2 - w(\alpha\alpha_2)) + \cdots \\ &\quad + (n - 2 - w(\alpha\alpha_{n-2})) + (n - w(\alpha\alpha_{n-1})) \\ &= 2 + 2n + (n-3)(n-2) - C_N\end{aligned}$$

which gives the desired formula (4.1). □

We can now use Theorem 4.1 to obtain the following result on the complexity of self-dual normal bases over GF(2).

Theorem 4.2. *Let* $n \equiv 2 \bmod 4$, *and let* N *be a self-dual normal basis for* $\mathrm{GF}(2^n)/\mathrm{GF}(2)$. *Then one has*

$$2n - 1 \leq C_N \leq n^2 - 5n + 9. \tag{4.9}$$

Equality holds in one of these bounds if and only if either N *or* N^* *is optimal; in particular, this implies that* $2n + 1$ *is a prime and that* 2 *is a primitive root* $\bmod 2n + 1$.

Proof. The lower bound in (4.9) holds for any normal basis, by Result 1.1. Since N is self-dual, so is the normal basis N^* constructed in Corollary 3.3. We note that $(N^*)^* = N$; hence we may apply Theorem 4.1 to N^* and obtain

$$C_N = n^2 - 3n + 8 - C_{N^*} \leq n^2 - 3n + 8 - (2n - 1) \tag{4.10}$$

which gives the upper bound in (4.9). Obviously, equality in one of the two bounds means that either N or N^* is optimal. By Theorem 2.5, either N or N^* is constructed as in Result 1.3, and so $2n + 1$ is prime and one of the conditions (1.9) and (1.10) must be satisfied. But $2n + 1 \equiv 1 \bmod 4$ (since n is even) which rules out condition (1.10). □

Mullin, Onyszchuk, Vanstone and Wilson [20] have conducted computer searches of normal bases in order to determine the maximum and minimum complexities for $n \leq 30$. (For $n = 28, 29, 30$, they only have lower bounds on the maximum complexity, since the number of normal bases was too large for complete computer searches in these cases. The lower bounds are exact, since there are optimal normal bases in all three cases.) It turns out to be interesting to compare our results on the values $n \equiv 2 \bmod 4$ with the relevant cases in their table.

Example 4.3. We note that the upper bound in (4.9) agrees with the maximum complexity of *any* normal basis in the cases $n = 2$, 14, 18, 26. Moreover, in each of these cases Result 1.3 yields a self-dual optimal normal basis N so that the corresponding self-dual basis N^* will by Theorem 4.1 achieve the maximum complexity.

Example 4.4. For $n = 30$, Result 1.3 also yields an optimal normal basis; then Theorem 4.1 gives a self-dual normal basis of complexity 759. This is also quite interesting, since the largest complexity found by the incomplete computer search of [20] is only 587. (There are 11059200 normal bases for $n = 30$.)

Example 4.5. The bound in (4.9) does not always yield a normal basis of maximum complexity, though. For $n = 6$ the upper bound in (4.9) is only 15 (which may be realized using an optimal normal basis in Theorem 4.1). However, the table of [20] shows that the maximum complexity among the 4 normal bases for $n = 6$ is 17. For

$n = 10$, there is no self-dual normal basis meeting the upper bound 59 in Theorem 4.2, since 21 is not a prime. Since a self-dual normal basis has odd complexity by Corollary 2.4, the largest conceivable complexity for a self-dual normal basis for $n = 10$ is 57. But according to [20] there is a normal basis of complexity 61 among the 48 normal bases for $n = 10$.

The preceding examples leave the case $n = 22$. In Section 5, we will also be able to construct a self-dual normal basis of maximum complexity in this case.

As Example 4.5 shows, the assumption of self-duality is important in Theorems 4.1 and 4.2. For a general normal basis N (with $q = 2$ and n even) it is not known how the complexities of N and N^* are related. As a further application of the present techniques, we shall settle this question in the case where N is one of the optimal normal bases constructed in Result 1.2; it turns out that in this case N^* has low complexity, too.

Theorem 4.6. *Let $n + 1$ be a prime, assume that 2 is a primitive root modulo $n + 1$, and let N be the optimal normal basis for $\mathrm{GF}(2^n)/\mathrm{GF}(2)$ consisting of the n primitive $(n + 1)$-st roots of unity (as in Result 1.2). Then the basis N^* constructed as in Corollary 3.3 has complexity*

$$C_{N^*} = 3n - 3. \tag{4.11}$$

Proof. Since the elements of N now are the nonunit elements of the group of $(n + 1)$-st roots of unity, it is clear that all but one of the products $\alpha\alpha_i$ have weight 1; the exception occurs for the unique index k with $\alpha_k = \alpha^{-1}$ in which case $\alpha\alpha_k = 1 = \mathrm{Tr}(\alpha)$ has weight n. Since the basis N^* is generated by $\gamma = 1 + \alpha$, we again have

$$\gamma\gamma_i = (1 + \alpha)(1 + \alpha_i) = 1 + \alpha + \alpha_i + \alpha\alpha_i. \tag{4.12}$$

In case $i = k$, (4.12) reduces to $\gamma\gamma_k = \alpha + \alpha_k$, and thus we have

$$w(\gamma\gamma_k) = 2. \tag{4.13}$$

For $i \neq k$, we have $\alpha\alpha_i = \alpha_j$ for the appropriate index $j = j(i)$; clearly, one has $j \neq 0, i$. Thus (4.12) can be written as

$$\gamma\gamma_i = 1 + \alpha + \alpha_i + \alpha_j = \gamma_0 + \gamma_i + \gamma_j \quad \text{for } i \neq k. \tag{4.14}$$

This shows that

$$w(\gamma\gamma_i) = 3 \quad \text{for } i \neq 0, k \tag{4.15}$$

and, of course, $w(\gamma\gamma_0) = 1$. Altogether, we obtain the desired result $C_{N^*} = 3n - 3$. □

Reviewing the proofs of Theorems 4.1 and 4.6, it seems difficult to obtain a general result relating the complexities of N and N^* for an arbitrary normal basis N, since the unknown distribution of both even and odd weights among the $\alpha\alpha_i$ presumably

prevents the required computations. It is also an open problem whether anything similar can be done in the case of odd characteristic.

5. A product construction for normal bases

In this final section, we generalize a product construction for normal basis generators due to Séguin [21] for $q = 2$ to arbitrary prime powers. Moreover, we strengthen his results by also including information about the behaviour of the trace function under this construction; in particular, we shall see that it preserves trace-orthogonality. We first state a lemma.

Lemma 5.1. *Let $A = \{\alpha_0, \dots, \alpha_{m-1}\}$ and $B = \{\beta_0, \dots, \beta_{n-1}\}$ be bases for $K = \mathrm{GF}(q^m)$ and $L = \mathrm{GF}(q^n)$ over $F = \mathrm{GF}(q)$, respectively, and assume that m and n are coprime. Then $C = \{\alpha_i\beta_j: i = 0, \dots, m-1, j = 0, \dots, n-1\}$ is a basis for $\mathrm{GF}(q^{mn})$ over F.*

Proof. Without loss of generality, we may assume that both K and L are subfields of $E = \mathrm{GF}(q^{mn})$. Now the set E' of all F-linear combinations of the mn elements in C is easily seen to be a subring and hence a subfield of E. One also sees that E' contains both K and L which are extensions of degree m and n of F, respectively. Therefore the degree of E' must be at least mn (since m and n are coprime by hypothesis), and thus we have $E = E'$. This shows that C is indeed a basis of E. □

Theorem 5.2. *Let α and β generate normal bases A and B for $K = \mathrm{GF}(q^m)$ and $L = \mathrm{GF}(q^n)$ over $F = \mathrm{GF}(q)$, respectively. Assume that m and n are coprime and put $\gamma = \alpha\beta$. Then one has the following:*

$$\gamma \text{ generates a normal basis } N \text{ for } E = \mathrm{GF}(q^{mn}) \text{ over } F; \tag{5.1}$$

$$C_N = C_A C_B; \tag{5.2}$$

$$\mathrm{Tr}_{E/F}(\xi\eta) = \mathrm{Tr}_{K/F}(\xi)\,\mathrm{Tr}_{L/F}(\eta) \text{ for all } \xi \in K \text{ and } \eta \in L; \tag{5.3}$$

$$\text{if both } A \text{ and } B \text{ are trace-orthogonal, then } N \text{ is also trace-orthogonal.} \tag{5.4}$$

Proof. Write $A = \{\alpha_0, \dots, \alpha_{m-1}\}$ and $B = \{\beta_0, \dots, \beta_{n-1}\}$. Then $N = \{\alpha_i\beta_j: i = 0, \dots, m-1, j = 0, \dots, n-1\}$ is a basis for E/F by Lemma 5.1. We now claim that N actually consists of the conjugates of $\gamma = \alpha\beta$ under the Galois group G of E/F, i.e., the elements

$$\gamma^{q^h} = \alpha^{q^h}\beta^{q^h} \quad \text{with } h = 0, \dots, mn-1. \tag{5.5}$$

Note that $\alpha^{q^h} = \alpha^{q^c}$ and $\beta^{q^h} = \beta^{q^d}$, where c and d are obtained by reducing h modulo m and n, respectively. Thus the elements in (5.5) can also be written as

$$\alpha^{q^c}\beta^{q^d} \quad \text{with } c = 0, \dots, m-1 \text{ and } d = 0, \dots, n-1. \tag{5.6}$$

But the α^{q^c} are the conjugates of α (i.e., the elements of A), and the β^{q^d} are the conjugates of β (i.e., the elements of B). Hence N indeed consists of the conjugates of γ and is therefore a normal basis for E/F, proving the validity of (5.1).

Now let

$$\xi = x_0\alpha_0 + \cdots + x_{m-1}\alpha_{m-1} \quad \text{and} \quad \eta = y_0\beta_0 + \cdots + y_{n-1}\beta_{n-1} \tag{5.7}$$

be any two elements of K and L, respectively. Then

$$\xi\eta = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} x_i y_j \alpha_i \beta_j \tag{5.8}$$

is the representation of $\xi\eta$ with respect to the basis N. Recall that the complexity C_N of N is the sum of the weights of all the products $\gamma\gamma^{q^h}$ $(h = 0, \ldots, mn-1)$, i.e., of all the products

$$(\alpha\beta)(\alpha_i\beta_j) = (\alpha\alpha_i)(\beta\beta_j) \quad \text{with } i = 0, \ldots, m-1 \text{ and } j = 0, \ldots, n-1. \tag{5.9}$$

Applying (5.8) to $\xi = \alpha\alpha_i$ and $\eta = \beta\beta_j$, we immediately see that the weight of $(\alpha\beta)(\alpha_i\beta_j)$ is the product of the weights of $\alpha\alpha_i$ and $\beta\beta_j$. In view of the ranges of i and j and (5.9), this implies the validity of (5.2).

We now apply formula (1.12) to the elements ξ and η in (5.7) and to their product in (5.8), taking into account the fact that the $\alpha_i\beta_j$ are the conjugates of γ. We obtain the following equations:

$$\mathrm{Tr}_{K/F}(\xi) = (x_0 + \cdots + x_{m-1})\,\mathrm{Tr}_{K/F}(\alpha); \tag{5.10}$$

$$\mathrm{Tr}_{L/F}(\eta) = (y_0 + \cdots + y_{n-1})\,\mathrm{Tr}_{L/F}(\beta); \tag{5.11}$$

$$\mathrm{Tr}_{E/F}(\xi\eta) = (x_0y_0 + \cdots + x_{m-1}y_{n-1})\,\mathrm{Tr}_{E/F}(\gamma). \tag{5.12}$$

These three equations immediately imply the validity of the product formula (5.3) provided that we can show that the special case

$$\mathrm{Tr}_{E/F}(\gamma) = \mathrm{Tr}_{K/F}(\alpha)\,\mathrm{Tr}_{L/F}(\beta) \tag{5.13}$$

holds. Using (5.1), this is easily checked:

$$\begin{aligned}\mathrm{Tr}_{E/F}(\gamma) &= \sum_{h=0}^{mn-1} \gamma^{q^h} = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \alpha_i\beta_j \\ &= \left(\sum_{i=0}^{m-1} \alpha^{q^i}\right)\left(\sum_{j=0}^{n-1} \beta^{q^j}\right) = \mathrm{Tr}_{K/F}(\alpha)\,\mathrm{Tr}_{L/F}(\beta).\end{aligned}$$

Finally, applying (5.3) to the products $\gamma\gamma_h$ $(h = 0, \ldots, mn-1)$, i.e., the products $(\alpha\alpha_i)(\beta\beta_j)$ with $i = 0, \ldots, m-1$ and $j = 0, \ldots, n-1$, immediately yields (5.4). □

We now give the example already announced in the preceding section.

Example 5.3. Let $q = 2$. By Results 1.2 and 1.3, there exist self-dual optimal normal

bases for the degrees $m = 2$ and $n = 11$. Thus there also exists a self-dual normal basis N with complexity $3 \times 21 = 63$ for the degree $k = 22$, by Theorem 5.2. Then the associated self-dual normal basis N^* has complexity 363, by Theorem 4.1. According to the tables of [20], these are the minimum and maximum complexities for normal bases of degree 22. This gives us one further example where our methods yield normal bases for the extremal cases.

Example 5.4. For $n = 10$ and $q = 2$, there are exactly 4 self-dual normal bases (cf. [4] or [10]). Our methods allow us to determine two of these bases and their complexities. By Results 1.2 and 1.3, there exist self-dual optimal normal bases for the degrees 2 and 5. Thus there also exists a self-dual normal basis N with complexity $3 \times 9 = 27$ for the degree 10, by Theorem 5.2. Then the associated self-dual normal basis N^* has complexity 51, by Theorem 4.1. For $n = 6$, there are exactly 2 self-dual normal bases, with complexities 11 and 15, respectively. One of them is the optimal normal basis N constructed in Result 1.3, and the other one can be obtained both as N^* (by Theorem 4.1) and also by the product construction of Theorem 5.2.

Example 5.5. As noted by Séguin [21], applying Theorem 5.2 for $q = 2$ produces normal bases with the minimum complexities (according to the tables in [20]) for each of the values $n = 15$, 20, 21, 22 and 24. Similarly, Theorem 5.2 also produces normal bases with the minimum complexity for $q = 3$ and $n = 12$ as well as for $q = n = 5$, cf. Tables 3.2 and 3.3 of Menezes [16].

References

[0] G.B. Agnew, R.C. Mullin and S.A. Vanstone, Fast exponentiation in GF(2^n), in: Advances in Cryptology – Eurocrypt '88, Lecture Notes in Computer Science 330 (Springer, Berlin, 1988) 251–255.

[1] G.B. Agnew, R.C. Mullin, I.M. Onyszchuk and S.A. Vanstone, An implementation for a fast public key cryptosystem, J. Cryptology 3 (1991) 63–79.

[2] D.W. Ash, I.F. Blake and S.A. Vanstone, Low complexity normal bases, Discrete Appl. Math. 25 (1989) 191–210.

[3] T. Beth, Generalizing the discrete Fourier transform, Discrete Math. 56 (1985) 95–100.

[4] T. Beth and W. Geiselmann, Selbstduale Normalbasen über GF(q), Arch. Math. 55 (1990) 44–48.

[5] T. Beth, W. Geiselmann and F. Meyer, Finding (good) normal bases in finite fields, ISSAC-91 (ACM, New York, 1991) 173–179.

[6] W. Diffie and M.E. Hellmann, New directions in cryptography, IEEE Trans. Inform. Theory 22 (1976) 644–654.

[7] W. Fumy, Orthogonal transform encoding of cyclic codes, AAECC-3, Lecture Notes in Computer Science 229 (Springer, Berlin, 1986) 131–134.

[8] W. Geiselmann and D. Gollmann, Symmetry and duality in normal basis multiplication, AAECC-6, Lecture Notes in Computer Science 357 (Springer, Berlin, 1989) 230–238.

[9] D. Gollmann, Algorithmenentwurf in der Kryptographie, Habilitationsschrift, FB Informatik, Universität Karlsruhe, Karlsruhe (1990).

[10] D. Jungnickel, A.J. Menezes and S.A. Vanstone, On the number of selfdual bases of GF(q^m) over GF(q), Proc. Amer. Math. Soc. 109 (1990) 23–29.

[11] A. Lempel, Characterization and synthesis of self-complementary normal bases in finite fields, Linear Algebra Appl. 98 (1988) 331–346.

[12] A. Lempel and G. Seroussi, Factorization of symmetric matrices and trace-orthogonal bases in finite fields, SIAM J. Comput. 9 (1980) 758–767.

[13] A. Lempel and M.J. Weinberger, Self-complementary normal bases in finite fields, SIAM J. Discrete Math. 1 (1988) 193–198.

[14] R. Lidl and H. Niederreiter, Introduction to Finite Fields and their Applications (Cambridge University Press, Cambridge, 1986).

[15] J.L. Massey and J.K. Omura, Computational method and apparatus for finite field arithmetic, U.S. Patent application (1981).

[16] A.J. Menezes, Representations in finite fields, M. Math. Thesis, University of Waterloo, Waterloo, Ont. (1989).

[17] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, Some computational aspects of root finding in GF(q^m), ISSAC'88, Lecture Notes in Computer Science 358 (Springer, Berlin, 1989) 259–270.

[18] F. Meyer, Normalbasismultiplikation in endlichen Körpern, Diplomarbeit, Universität Karlsruhe, Karlsruhe (1990).

[19] R.C. Mullin, A characterization of the extremal distributions of optimal normal bases, in: D. Jungnickel and S.A. Vanstone, eds., Coding Theory, Design Theory, Group Theory (Wiley, New York, 1993) 41–49.

[20] R.C. Mullin, I.M. Onyszchuk, S.A. Vanstone and R.M. Wilson, Optimal normal bases, Discrete Appl. Math. 22 (1988/89) 149–161.

[21] J.E. Séguin, Low complexity normal bases, Discrete Appl. Math. 28 (1990) 309–312.